BROKER-BASED INTERWORKING USING HIERARCHICAL CERTIFICATES

BACKGROUND OF THE INVENTION

FIELD OF THE INVENTION

The present invention generally relates to networking and, more particularly, to broker-based interworking Authentication, Authorization and Accounting (AAA) using hierarchical certificates.

BACKGROUND OF THE INVENTION

Typically, Authentication, Authorization and Accounting (AAA) are required to access and utilize networks such as cellular networks and Wireless Local Area Networks (WLANs). In an environment in which a mobile terminal has multiple network access mechanisms, providing AAA interworking among these networks is of great importance. However, it is generally the case that the involved networks do not belong to the same administrative domain and do not share the same AAA schemes. Moreover, it is difficult for a cellular operator to establish a contract relationship with each and every wireless LAN operator and vice versa. Further, the mobile user that has signed up for interworking should not be aware of any third party involved in the interworking, i.e. they only need to maintain a single account, i.e., their own cellular account.

There are two main types of interworking between cellular networks and WLANs: tight coupling and loose coupling. In a loose coupling scenario, the WLAN and the cellular network have independent data paths but the AAA for WLAN users relies on cellular network AAA functions. However, the cellular network AAA protocols (MAP/SS7) are incompatible with Internet Protocol (IP) based protocols used by WLAN users.

To address the problems of the networks not belonging to the same administrative domain and of not sharing the same AAA schemes, special interworking functions or gateways were proposed to bridge between cellular network and WLAN AAA schemes. Some of these special functions require that the cellular network Home Location Register (HLR) be adapted; however, this is not desirable for many reasons, particularly from the perspective of the cellular operators.

Conventional broker models directed to the problem of establishing contracts between each and every WLAN and cellular network operator all require that the broker deploy AAA engines that are involved in mobile user authentication in real-time; this easily creates a single point of failure. Some of these broker models also require that a mobile user create a separate account with the broker; this is quite inconvenient for the user.

Accordingly, it would be desirable and highly advantageous to have an interworking AAA scheme that overcomes the above-described problems of prior art interworking AAA schemes.

SUMMARY OF THE INVENTION

The problems stated above, as well as other related problems of the prior art, are solved by the present invention, broker-based interworking Authentication, Authorization and Accounting (AAA) using hierarchical certificates.

The present invention is particularly useful for, but is not limited to, the loose coupling scenario in cellular data network and WLAN interworking. By deploying a broker, the cellular operators do not have to establish a contract relationship with each and every wireless LAN operator for interworking. It is thus much more scalable than prior art approaches. Further, by using hierarchical certificates, the broker does not have to maintain any mobile user information. Mobile users can just use their cellular account to get access to wireless LANs having contracts with their cellular operators.

According to an aspect of the present invention, there is provided a method for Authentication Authorization and Accounting (AAA) in an interworking between at least two networks. The at least two networks are capable of communicating with a broker and include a first network and a second network. The second network receives a broker public key from the broker and a first network to user certificate from a user device corresponding to a user of the first network. The first network to user certificate is signed by a first network private key and includes a broker to first network certificate and a user public key. The broker to first network certificate is signed by a broker private key and includes a first network public key. A session key is sent from the second network to the user device when the broker to first network certificate and the first network to user certificate are determined to be authentic by the second network based upon the broker public key and the first network public key, respectively. The session key is encrypted with the user public key. The

session key is used for permitting the user device to access the second network.

These and other aspects, features and advantages of the present invention will become apparent from the following detailed description of preferred embodiments, which is to be read in connection with the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a block diagram illustrating a computer system 100 to which the present invention may be applied, according to an illustrative embodiment of the present invention;

FIG. 2 is a block diagram illustrating a communication structure to which the present invention may be applied, according to an illustrative embodiment of the present invention;

FIG. 3 is a flow diagram illustrating a broker-based method for Authentication Authorization and Accounting (AAA) of a mobile user in a loose coupling interworking between access networks, according to an illustrative embodiment of the present invention; and

FIG. 4 is a flow diagram illustrating a certificate based method for Authentication Authorization and Accounting (AAA) of a mobile user in a loose coupling interworking between access networks, according to another illustrative embodiment of the present invention.

DETAILED DESCRIPTION OF THE INVENTION

The present invention is directed to broker-based interworking Authentication, Authorization and Accounting (AAA) using hierarchical certificates. It is to be appreciated that the present invention is applicable to any combination of access networks. However, the present invention is particularly applicable to cellular network and Wireless Local Area Network (WLAN) interworking.

It is to be understood that the present invention may be implemented in various forms of hardware, software, firmware, special purpose processors, or a combination thereof. Preferably, the present invention is implemented as a combination of hardware and software. Moreover, the software is preferably implemented as an application program tangibly embodied on a program storage device. The application program may be uploaded to, and executed by, a machine comprising any suitable architecture. Preferably, the machine is implemented on a computer platform having hardware such as one or more central processing units (CPU), a random access memory (RAM), and input/output (I/O) interface(s). The

computer platform also includes an operating system and microinstruction code. The various processes and functions described herein may either be part of the microinstruction code or part of the application program (or a combination thereof) which is executed via the operating system. In addition, various other peripheral devices may be connected to the computer platform such as an additional data storage device and a printing device.

It is to be further understood that, because some of the constituent system components and method steps depicted in the accompanying Figures are preferably implemented in software, the actual connections between the system components (or the process steps) may differ depending upon the manner in which the present invention is programmed. Given the teachings herein, one of ordinary skill in the related art will be able to contemplate these and similar implementations or configurations of the present invention.

FIG. 1 is a block diagram illustrating a computer system 100 to which the present invention may be applied, according to an illustrative embodiment of the present invention. Computer system 100 may be implemented, for example, in a mobile device used to access a wireless LAN or a cellular network, or an access point for implementing a wireless LAN, by including the necessary communications interface elements and processing elements as is known in the art. In the case of a mobile user device, computer system 100 would include, for example, the necessary radio interfaces for communicating with the required radio access networks, as well as the processing elements for encoding and decoding the messages according to the applicable standards. The computer processing system 100 includes at least one processor (CPU) 102 operatively coupled to other components via a system bus 104. A read only memory (ROM) 106, a random access memory (RAM) 108, a display adapter 110, an I/O adapter 112, a user interface adapter 114, a sound adapter 199, and a network adapter 198, are operatively coupled to the system bus 104.

A display device 116 is operatively coupled to system bus 104 by display adapter 110. A disk storage device (e.g., a magnetic or optical disk storage device) 118 is operatively coupled to system bus 104 by I/O adapter 112.

A mouse 120 and keyboard 122 are operatively coupled to system bus 104 by user interface adapter 114. The mouse 120 and keyboard 122 are used to input and output information to and from system 100.

At least one speaker (herein after "speaker") 197 is operatively coupled to system bus 104 by sound adapter 199.

A (digital and/or analog) modem 196 is operatively coupled to system bus 104 by network adapter 198.

The present invention provides an approach to AAA in which a broker is employed. The broker serves as a certificate authority instead of a real-time authentication engine. Thus, the broker is no longer a single point of failure. The broker issues certificates to the wireless networks which, in turn, issue their own certificates to individual mobile users subscribed to the interworking service.

FIG. 2 is a block diagram illustrating a communication structure to which the present invention may be applied, according to an illustrative embodiment of the present invention. In the illustrative embodiment of FIG. 2, the communication structure includes a cellular network 210, a Wireless Local Area Network (WLAN) 220, a broker 230, and a mobile user 240. The present invention provides a certificate based scheme to provide AAA services to WLAN users. As noted above, the present invention may be applied to any combination of networks, including different numbers and different types of networks.

FIG. 3 is a flow diagram illustrating a broker-based method for Authentication Authorization and Accounting (AAA) of a mobile user in a loose coupling interworking between access networks, according to an illustrative embodiment of the present invention. The access networks include a cellular network and a Wireless Local Area Network (WLAN). The cellular network is associated with at least a mobile user. It is to be appreciated that while the illustrative embodiment of FIG. 3 (as well as the illustrative embodiment of FIG. 4 below) is described with respect to a cellular network and a WLAN, any combination of networks, including the preceding and other types of networks as well as different numbers of networks (e.g., one cellular network and three WLANs, two cellular networks and two WLANs, and so forth), may be readily employed in accordance with the present invention while maintaining the spirit and scope of the present invention. It is to be further appreciated in preferred embodiments of the present invention, there will likely be a single cellular network to which the mobile user has initially contracted with for service, and a plurality of WLANs that have an interworking contract with the single cellular network. The interworking contract may be implemented with various known communications methods between the WLANs and the cellular network.

A public key K_{pub_b} of the broker is sent from the broker to the WLAN, the latter having an interworking contract with the cellular network (step 305). In the event that the cellular network has an interworking contract with more than one WLAN, then the broker could send the public key K_{pub_b} to all of these WLANs. It is preferable, but not mandatory, that the public key K_{pub_b} of the broker is sent via a secure channel so that the WLAN can be sure that the public key K_{pub_b} is indeed the public key of the broker.

A broker to cellular network certificate is issued to the cellular network by the broker (step 310). The broker to cellular network certificate includes, but is not limited to, the following: a public key K_{pub_cn} of the cellular network; and an ID of the cellular network. The broker to cellular network certificate is signed with a private key K_{pri_b} of the broker.

Upon a mobile user signing up with the cellular network for WLAN interworking service, a cellular network to mobile user certificate is issued to the mobile user by the cellular network (step 315). The cellular network to mobile user certificate includes, but is not limited to, the following: the broker to cellular network certificate; a public key K_{pub_m} of the mobile user; a mobile user subscription level (whether the mobile user is subscribed for WLAN interworking service); an expiration time of the cellular network to mobile user certificate. The cellular network to mobile user certificate is signed with a private key K_{pri_cn} of the cellular network.

Upon the mobile user moving into an area under coverage of the WLAN, the mobile user sends his/her certificate (i.e., the cellular network to mobile user certificate) to the WLAN (e.g., an Access Point (AP) or other entity of the WLAN) (step 320). It is determined by the WLAN whether the broker to cellular network certificate (included in the cellular network to mobile user certificate) is authentic, using the public key K_{pub_b} of the broker (sent to the WLAN at step 305) (step 325). If the broker to cellular network certificate is not authentic, then the method is terminated. However, if the broker to cellular network certificate is authentic, then the WLAN extracts the public key K_{pub_cn} of the cellular network (from the broker to cellular network certificate included in the cellular network to mobile user certificate) (step 330). Using the public key K_{pub_cn} of the cellular network, it is determined by the WLAN whether the cellular network to mobile user certificate is authentic (step 335).

If the cellular network to mobile user certificate is not authentic, then the method is terminated. However, if the cellular network to mobile user certificate is

authentic, then the WLAN extracts the public key K_{pub_m} of the mobile user from the cellular network to mobile user certificate and issues a session key to the mobile user that is encrypted with the public key K_{pub_m} of the mobile user (step 340). The session key may be, but is not limited to, a per user Wired Equivalent Privacy (WEP) key.

The encrypted session key is decrypted by the mobile user using his/her private key K_{pri_m} (step 345). The mobile user and the WLAN communicate using the session key (i.e., all subsequent communication between the mobile user and the WLAN is encrypted with the session key) (step 350). The mobile user is authenticated by the WLAN since only that specific mobile user has the necessary private key K_{pri_m} to decrypt the session key.

FIG. 4 is a flow diagram illustrating a certificate based method for Authentication Authorization and Accounting (AAA) of a mobile user in a loose coupling interworking between access networks, according to another illustrative embodiment of the present invention. The access networks include a cellular network and a Wireless Local Area Network (WLAN). The cellular network is associated with at least a mobile user. The method of FIG. 4 allows for mutual authentication between the mobile user and the WLAN, so that the mobile user can also verify that he/she is indeed talking to a legitimate WLAN (to prevent, e.g., messages from being snooped).

A public key K_{pub_b} of the broker and a broker to WLAN certificate are sent from the broker to the WLAN, the latter having an interworking contract with the cellular network (step 405). The broker to WLAN certificate includes, but is not limited to, the following: a public key K_{pub_w} of the WLAN; and an ID of the WLAN. The broker to WLAN certificate is signed with a private key K_{pri_b} of the broker.

In the event that the cellular network has an interworking contract with more than one WLAN, then the broker could send the public key K_{pub_b} to all of these WLANs. It is preferable, but not mandatory, that the public key K_{pub_b} of the broker is sent via a secure channel so that the WLAN can be sure that the public key K_{pub_b} is indeed the public key of the broker.

A broker to cellular network certificate is issued to the cellular network by the broker (step 410). The broker to cellular network certificate includes, but is not limited to, the following: a public key K_{pub_cn} of the cellular network; an ID of the cellular network; and a public key K_{pub_b} of the broker. The broker to cellular network certificate is signed with a private key K_{pri_b} of the broker.

Upon a mobile user signing up with the cellular network for WLAN interworking service, a cellular network to mobile user certificate is issued to the mobile user by the cellular network (step 415). The cellular network to mobile user certificate includes, but is not limited to, the following: the broker to cellular network certificate; a public key K_{pub_m} of the mobile user; a mobile user subscription level (whether the mobile user is subscribed for WLAN interworking service); an expiration time of the cellular network to mobile user certificate. The cellular network to mobile user certificate is signed with a private key K_{pri_cn} of the cellular network. The public key K_{pub_b} of the broker is also sent to the mobile user (step 417).

Upon the mobile user moving into an area under coverage of the WLAN, the mobile user sends his/her certificate (i.e., the cellular network to mobile user certificate) to the WLAN (e.g., an Access Point (AP) or other entity of the WLAN) (step 420). It is determined by the WLAN whether the broker to cellular network certificate (included in the cellular network to mobile user certificate) is authentic, using the public key K_{pub_b} of the broker (sent to the WLAN at step 405) (step 425). If the broker to cellular network certificate is not authentic, then the method is terminated. However, if the broker to cellular network certificate is authentic, then the WLAN extracts the public key K_{pub_cn} of the cellular network (from the broker to cellular network certificate included in the cellular network to mobile user certificate) (step 430). Using the public key K_{pub_cn} of the cellular network, it is determined by the WLAN whether the cellular network to mobile user certificate is authentic (step 435).

If the cellular network to mobile user certificate is not authentic, then the method is terminated. However, if the cellular network to mobile user certificate is authentic, the WLAN extracts the public key K_{pub_m} of the mobile user and issues a session key to the mobile user that is encrypted with the public key K_{pub_m} of the mobile user and is signed by a private key K_{pri_w} of the WLAN and also sends to the mobile user the broker to WLAN certificate that is signed by the private key K_{pri_b} of the broker (step 440). The broker to WLAN certificate includes a public key K_{pub_w} of the WLAN. The session key may be, but is not limited to, a per user Wired Equivalent Privacy (WEP) key.

It is determined by the mobile user whether the broker to WLAN certificate is authentic, using the public key K_{pub_b} of the broker (step 442). If the broker to WLAN certificate is not authentic, then the method is terminated. However, if the broker to WLAN certificate is authentic, then the public key K_{pub_w} of the WLAN is obtained by

the mobile user from the broker to WLAN certificate (step 443). It is determined by the mobile user whether the session key is authentic, using the public key K_{pub_w} of the WLAN (step 444). If the session key is not authentic, then the method is terminated.

However, if the session key is authentic, then the encrypted session key is decrypted by the mobile user using his/her private key K_{pri_m} (step 445). The mobile user and the WLAN communicate using the session key (i.e., all subsequent communication between the mobile user and the WLAN is encrypted with the session key) (step 450).

Although the illustrative embodiments have been described herein with reference to the accompanying drawings, it is to be understood that the present invention is not limited to those precise embodiments, and that various other changes and modifications may be affected therein by one skilled in the art without departing from the scope or spirit of the invention. For example, it is clear that the invention is applicable to any combinations of wireless and mobile communications networks, including, but not limited to those based on IEEE 802.11, Hiperlan 2, etc. All such changes and modifications are intended to be included within the scope of the invention as defined by the appended claims.